



MISSOURI DEPARTMENT OF MENTAL HEALTH

KEITH SCHAFER, DEPARTMENT DIRECTOR



DEPARTMENT
OPERATING
REGULATION
NUMBER

DOR
8.350

CHAPTER Regulation Compliance	SUBCHAPTER HIPAA Regulation	EFFECTIVE DATE July 1, 2008	NUMBER OF PAGES 5	PAGE NUMBER Page 1 of 5
SUBJECT Information Security Incidents		AUTHORITY Section 630.050	HISTORY See Below	
PERSON RESPONSIBLE Director, Information Technology Services Division			SUNSET DATE July 1, 2011	

PURPOSE: *The policy of the Missouri Department of Mental Health is to secure consumer's protected health information in compliance with federal law and federal regulations at 45 CFR Parts 160, 162, 164 and 42 CFR Part 2. This DOR establishes the normal day-to-day security activity and outlines what steps shall be taken in the event of an information security incident.*

APPLICATION: *Applies to Department of Mental Health, its facilities and workforce.*

(1) CONTENTS:

- (A) Definitions
- (B) Security Incident Handling
- (C) DMH INFOCON Procedures
- (D) INFOCON Measures
- (E) DOR Control
- (F) Sanctions
- (G) Review Process
- (H) Attachment

(2) DEFINITIONS

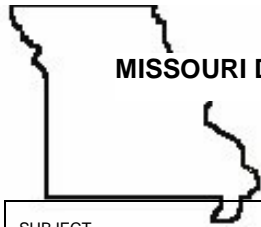
(A) The Information Operations Conditions (INFOCON). A structured, coordinated approach to defend against and react to adversarial attacks on State of Missouri Computer and Telecommunication networks and systems. The system was established as the Statewide standard for contingencies and countermeasures to scanning, probing, and other suspicious activity; unauthorized access; and data browsing.

(B) Computer Systems – Computers connected to local and statewide communication networks, database storage or electronic records systems, Internet or email or other DMH computing devices such as PDA's or stand-alone PC's.

(C) DMH Network – Electronic network allowing access to the DMH's personal computers, facility-based systems, and centrally-based systems (e.g. mainframe, server, desktop, etc.) and electronic data.

(D) Computer Network Attack – Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.

(E) DMH Workforce – Includes employees, volunteers, contract workers, interns, trainees and other persons who are in a DMH facility or Central Office on a regular



MISSOURI DEPARTMENT OF MENTAL HEALTH

KEITH SCHAFER, DEPARTMENT DIRECTOR



DEPARTMENT
OPERATING
REGULATION
NUMBER

DOR
8.350

SUBJECT	EFFECTIVE DATE	NUMBER OF PAGES	PAGE NUMBER
Information Security Incidents	July 1, 2008	2	Page 2 of 5

course of business. This shall include client workers employed by the DMH or any of its facilities.

(F) Chief Security Officer (CSO) – Individual designated by the DMH to oversee all activities related to the development, implementation, maintenance of, and adherence to Department and facility policies and procedures covering the electronic and physical security of, and access to, protected health information and other DMH data in compliance with federal and state laws and regulations.

(G) Local Security Officer (LSO) – Individual designated by a facility CEO to oversee facility information and physical security practice and policy compliance and to coordinate those activities with the Chief Security Officer.

(H) Security Incident – Means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

(I) Information Security Management Office (ISMO) -The Unit at the State of Missouri's Office of Administration responsible for monitoring the State of Missouri Computer network and notifying agencies of the State of Missouri's INFOCON level.

(3) Security Incident Handling

(A) Objectives:

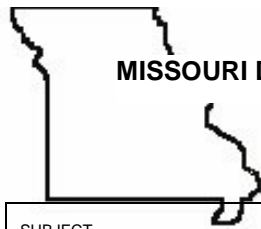
1. Ensure that all responsible parties have clear understanding about the tasks they should perform during an incident;
2. Ensure that there is prompt recovery for the compromised system;
3. Minimize the possible impact of the incident in terms of information leakage, corruption and system disruption etc.;
4. Prevent further attacks and damages; and
5. Deal with related legal issues.

(B) Security incidents may include but are not limited to:

1. Accidental user error;
2. Improper use of access privileges;
3. Employee access to damage or steal information;
4. Physical breach;
5. External breach to illegally access information; and
6. Technical breach impacting operations of compromising systems or information.

(C) Examples of incidents that shall be reported are:

1. Attempts to gain unauthorized access to systems or data;
2. Unwanted disruption or denial of service;
3. The unauthorized use or access of a system for transmission, processing or storage, exploitation tool placement, or degradation of data;
4. Changes to system hardware, firmware, and/or usage of software characteristics without the knowledge, instruction, or consent of the CSO or LSO;
5. Discovery of malicious code which includes, but is not limited to, worms, viruses, Trojans, web defacement, etc.; and



MISSOURI DEPARTMENT OF MENTAL HEALTH

KEITH SCHAFER, DEPARTMENT DIRECTOR



DEPARTMENT
OPERATING
REGULATION
NUMBER

DOR
8.350

SUBJECT	EFFECTIVE DATE	NUMBER OF PAGES	PAGE NUMBER
Information Security Incidents	July 1, 2008	3	Page 3 of 5

6. Any breach of the computing environment that has the potential to spread outside of the agency's immediate control.

(D) Each DMH facility shall have a Security Incident Plan outlining the following.

1. Scope – define the functional area for which the individual(s) will be responsible. It may be the whole region, office, specific IT system or application. Plans are to be completed and approved by the CSO no later than April 1, 2005.

2. Establish Goals and Priorities

A. Goals shall include:

(I) returning the system to normal operation in shortest time possible;

(II) Minimize the impact to other systems;

(III) Avoid further incidents;

(IV) Identify the root cause;

(V) Assess the impact and damage of the incident;

(VI) Collect evidence to support subsequent case investigation; and

(VII) Where applicable, track disclosures as prescribed in DOR 8.060.

B. Priorities shall include:

(I) Protect sensitive or Critical Resources;

(II) Protect important data which are costly when lost or damaged;

(III) Minimize disruption of service; and

(IV) Protect public image of the Department.

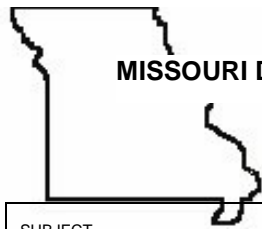
3. Clearly define the roles/responsibilities of all parties participating in the security incident handling process. Examples include: listing the responsible party for viruses, malicious code attacks, unauthorized access and denial of resources. In addition, include the responsible parties' role regarding the incident whether they are primarily responsible for overseeing, performing actions listed on DMH INFOCON Measures Spreadsheet or documenting.

4. List any constraints that may affect the result of security incident handling process. For example, it may be necessary to acquire external advice in areas lacking internal technical expertise.

(E) Security Incident Documentation. Whenever a security incident occurs, the LSO shall be responsible for the completion of the Report Of Security Incident form attached to this DOR. Where applicable, the LSO shall copy facility HR. LSO's are encouraged to discuss security incidents with CSO at the time of occurrence. The form shall be kept by the LSO for at least six (6) years or until all questions and/or legal actions are completed whichever is later.

(4) INFOCON Measures

(A) State of Missouri INFOCON levels focus on computer network based information system intrusion consistent with the risk of impact to sustaining



MISSOURI DEPARTMENT OF MENTAL HEALTH

KEITH SCHAFER, DEPARTMENT DIRECTOR



DEPARTMENT
OPERATING
REGULATION
NUMBER

DOR
8.350

SUBJECT	EFFECTIVE DATE	NUMBER OF PAGES	PAGE NUMBER
Information Security Incidents	July 1, 2008	4	Page 4 of 5

operations through the intentional disruption of information systems. INFOCON levels are:

1. Normal activity;
2. Increased risk of attack;
3. Specific risk of attack;
4. Limited attack; and
5. General attack.

(B) Countermeasures at each level includes preventive actions, actions taken during an attack, and damage control/mitigating actions. See the DMH INFOCON Measures spreadsheet at DMH Online for more detailed information.

(5) DMH INFOCON Procedures

(A) Determining the INFOCON level. There are three broad categories of factors that influence the INFOCON level: operational, technical, and intelligence, including law enforcement intelligence. The INFOCON level is based on significant changes in one or more of them.

(B) Declaring INFOCON level

1. The ISMO will recommend changes in State of Missouri INFOCON levels to the agencies. Notice of a change in the State INFOCON level will be disseminated through ISMO's existing Incident Response Plan and Procedures. DMH is responsible for assessing the situation and establishing the appropriate INFOCON level based on evaluation of all relevant factors.

2. The DMH may change its INFOCON level from that declared by the ISMO; however, DMH shall remain at least as high as the current level recommended by the ISMO. The DMH CSO is responsible for assessing the situation and determining the proper DMH INFOCON level. DMH facilities shall maintain their INFOCON level equal to that of Central Office.

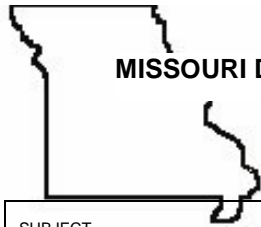
(C) Response Measures. Response measures associated with INFOCON levels are recommended actions. Ideally, operations will be based on advanced warning of an attack. Measures shall be commensurate with the risk, the adversary's assessed capability and intent (if known), and mission requirements.

(D) Reporting. Technical reporting shall be accomplished according to the State of Missouri Incident Response Plan and Procedures (maintained by ISMO). DMH shall also report violations of the law, such as unauthorized access to sustaining computer networks and systems, to the applicable law enforcement agency.

1. Reporting Channels. The DMH CSO shall report INFOCON level changes and summary reports to the ISMO and the LSO's at DMH facilities as appropriate.

2. Reporting Frequency. The CSO shall report INFOCON level changes and summary reports to the ISMO and the LSO's at DMH facilities as appropriate.

3. Report Formats. Reports of changes in INFOCON level shall be accompanied by an operational assessment of the situation when appropriate, and shall include:



MISSOURI DEPARTMENT OF MENTAL HEALTH

KEITH SCHAFER, DEPARTMENT DIRECTOR



DEPARTMENT
OPERATING
REGULATION
NUMBER

DOR
8.350

SUBJECT	EFFECTIVE DATE	NUMBER OF PAGES	PAGE NUMBER
Information Security Incidents	July 1, 2008	5	Page 5 of 5

A. For all INFOCON levels: organization and location, date, time of report, current INFOCON, reason for declaration of this INFOCON level, response actions taken, point of contact (name, title, contact information; and

B. INFOCON FOUR and FIVE: All of the above, plus: systems affected (network, classification, application, database/data file), degree to which

operational functions are affected, actual and/or potential impact on general capabilities, restoration priorities, workarounds.


(6) There shall be no facility policies pertaining to this topic. The Department Operating Regulations shall control

(7) Sanctions. Failure of workforce members to comply or ensure compliance with the DOR may result in disciplinary action, up to and including dismissal.

(8) Review Process. The Chief Security Officer may collect summaries of security incidents from each facility during the month of April each year beginning 2006 for the purpose of providing feedback to the Director, Office of information Systems and the Executive Team regarding trends and issues associated with compliance with this regulation. The LSO shall also establish thresholds and criteria for periodic review and analysis of information and data related to this DOR. At a minimum, routine review of patterns, outliers or unusual behavior related to access and security shall be conducted.

(9) Attachment: Form to record security incidents.

HISTORY: Original DOR effective September 1, 2004. On July 1, 2008 the sunset date was extended to July 1, 2011. Amendment effective July 1, 2008.

	Missouri Department of Mental Health Information Technology Report of Security Incident Facility Name _____	Local Security Officer Use Only: Local Security Officer Signature: _____ Received Date: _____
I. Instructions: <i>This form shall be used to report any acts or omissions that result in (1) the attempted or successful unauthorized access, use, disclosure, modification or destruction of information; or (2) interference with system operations in an information system.</i>		
II. Type of Incident		III. Date & Time of Incident
IV. System Compromised/Damage Caused		
V. Employee(s) Involved:		
VI. Initial Action Taken:	VII. Remedy Implemented:	
VIII. Remedy Date:		
IX. Date Reported to Local Security Officer:		
X. Person Reporting: _____ Work Location: _____ <div style="text-align: center;"><i>Signature</i></div>		
<i>When completed, please send to the Local Security Officer for further investigation and actions if necessary.</i>		
SECTION BELOW FOR USE BY LOCAL SECURITY OFFICER		
XI. FOLLOW UP ACTION BY LSO:		
XII. Date Reported to Superintendent:		
XII. Date Reported to HIPAA Privacy Officer:		
XIV. Local Security Officer Signature: _____		
<i>Documentation of investigation by Local Security Officer should be attached.</i>		
SECTION BELOW FOR USE BY HUMAN RESOURCES		
XV. Personnel Action Taken (Punitive, Probationary or Written plan of Probation):	XVI. Date Personnel Action Taken:	